

# 7. Seguridad en redes inalámbricas

Proceso

78%



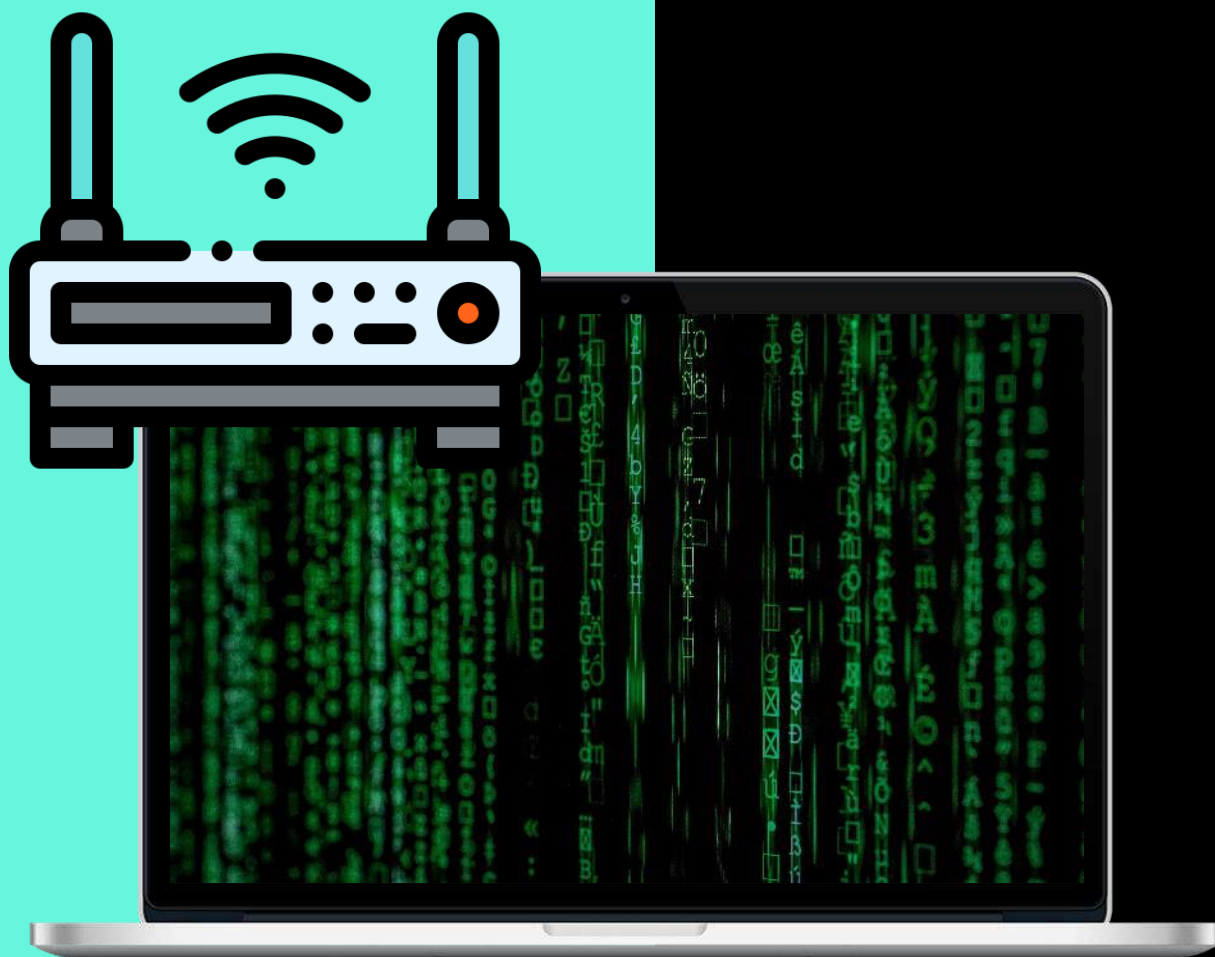
# Índice

- 7.1. **Introducción**
- 7.2. **Introducción al estándar inalámbrico 802.11 WIFI**
- 7.3. **Topologías**
- 7.4. **Seguridad en redes Wireless. Redes abiertas**
- 7.5. **WEP**
- 7.6. **WEP. Ataques**
- 7.7. **Otros mecanismos de cifrado**





## 7.1. Introducción



# Introducción.

Desde hace tiempo las redes inalámbricas (Wireless Networks, **WLAN**) están entre nosotros. Estas se han ido popularizando, tanto en lugares públicos y empresas como en hogares, gracias al creciente auge de los dispositivos móviles y los portátiles.

**Es cada vez más importante tomar conciencia de la seguridad en los entornos inalámbricos.**



Nos permiten tener movilidad total dentro del área de cobertura de red, tanto de usuarios como de equipos, ofreciendo servicios de comunicación de voz y datos.

Hay que destacar que la mayoría de los ataques que reciben las redes inalámbricas se efectúan desde la red interior.

**Su seguridad requiere de los siguientes servicios.**



### Autenticación

El proceso por el cual un usuario se asocia a una WLAN es lo que denominamos autenticación en el caso de las redes inalámbricas, ya que solo tras un correcto proceso se permitirá dicha asociación.



### Confidencialidad

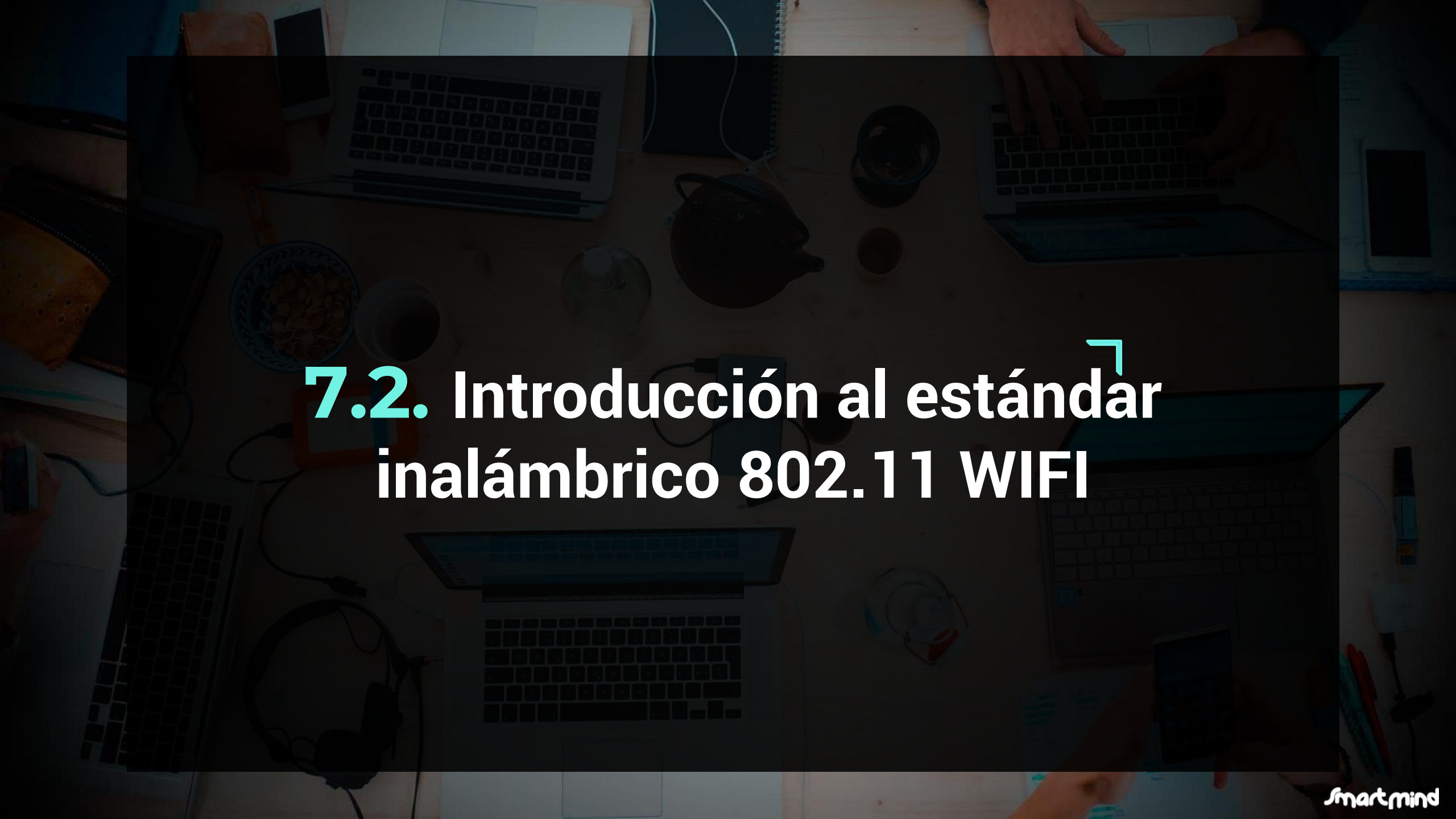
En las redes inalámbricas nos valemos de algoritmos criptográficos para asegurarnos la confidencialidad. Los más utilizados en la actualidad son el RC4 (**WEP**) y AES (**WPA2**).



### Gestión de claves

Como su propio nombre dice, dicho servicio se refiere a la generación de claves y su distribución.





## 7.2. Introducción al estándar inalámbrico 802.11 WIFI

# La especificación IEEE 802.11 es un estándar internacional que define las características de una red local inalámbrica o WLAN.

WIFI (Wireless Fidelity o fidelidad inalámbrica) es el nombre de la certificación que otorga Wi-Fi Alliance quien garantiza la compatibilidad entre dispositivos que utilizan el estándar 802.11.

Es habitual que la gente confunda el nombre del estándar con el de la certificación, pero hay que dejar muy claro que una red Wi-Fi es una red que cumple con el estándar 802.11.

A los dispositivos certificados por Wi-Fi Alliance, se les permite el uso del siguiente logotipo.






Como ya sabemos con WIFI se pueden crear redes de área local inalámbricas siempre y cuando el dispositivo en cuestión no esté muy alejado del punto de acceso. También hoy en día, los proveedores de Wi-Fi cubren áreas de gran concentración de usuarios. Dichas zonas se llaman “zonas locales de cobertura”.



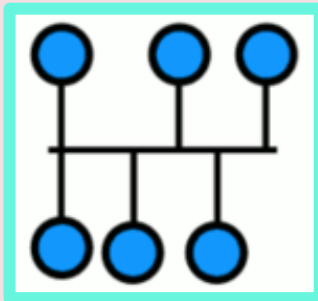




## 7.3. Topologías

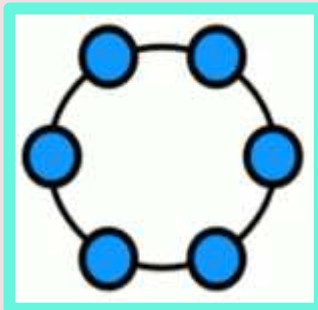


**El concepto de red puede definirse como conjunto de nodos interconectados.** Dependiendo de la forma en que estén conectados esos nodos, sea en el plano físico o lógico, podemos distinguir, entre otras, las siguientes topologías:



### Bus

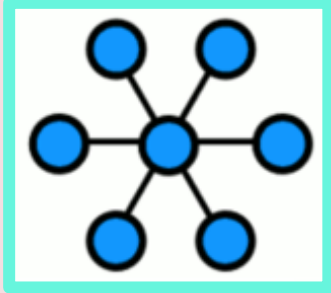
Todos los dispositivos comparten el mismo canal (bus) para comunicarse entre sí.



### Anillo

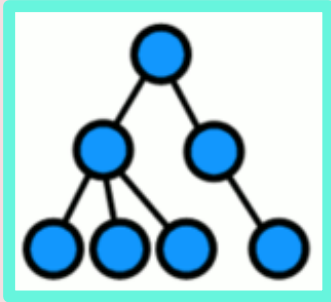
Cada estación tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente estación.





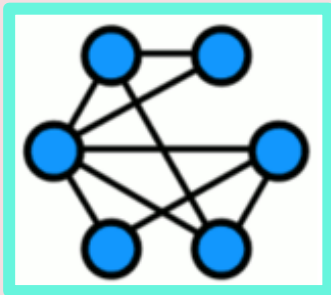
## Estrella

Las estaciones están conectadas directamente a un punto central y todas las comunicaciones se hacen a través de ese punto.



## Árbol

Los nodos están colocados en forma de árbol. Desde una visión topológica es parecida a una serie de redes en estrella interconectadas, salvo en que no tiene un concentrador central.



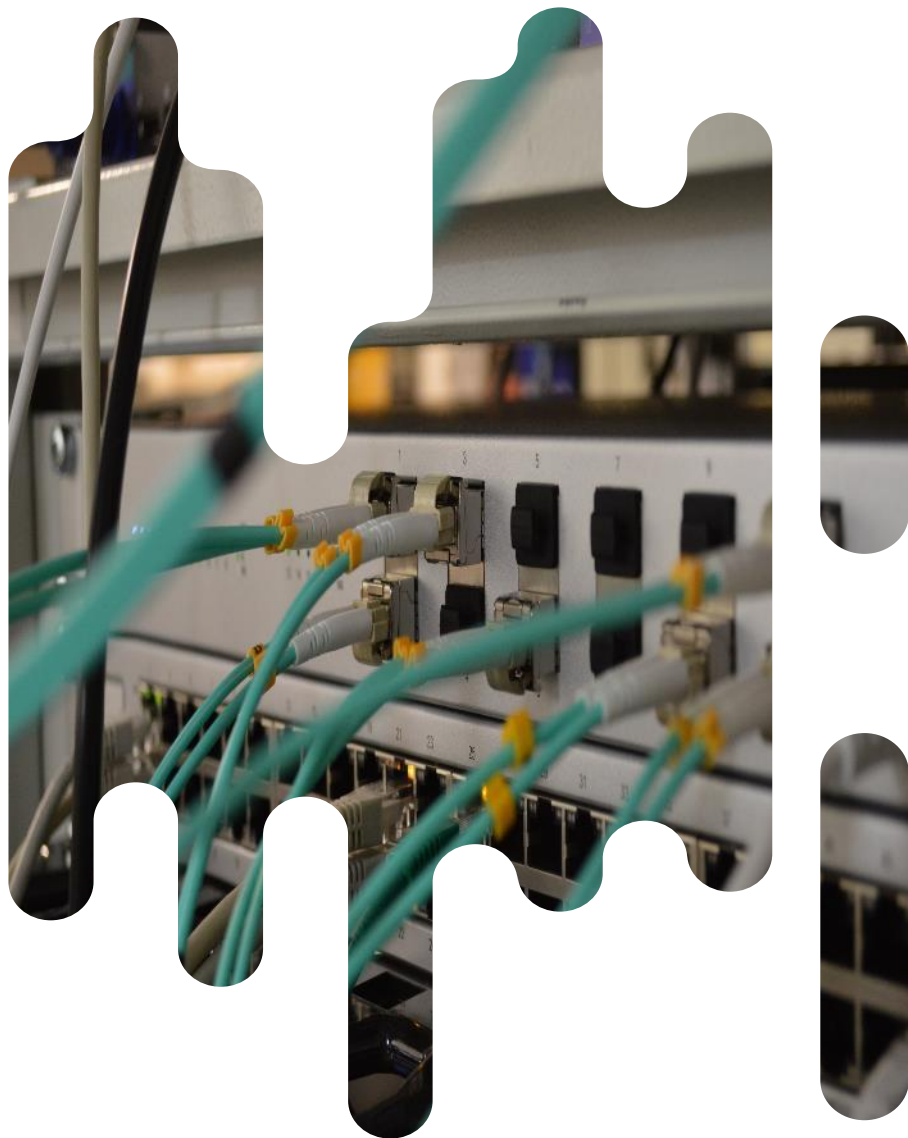
## Malla

Cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por distintos caminos.





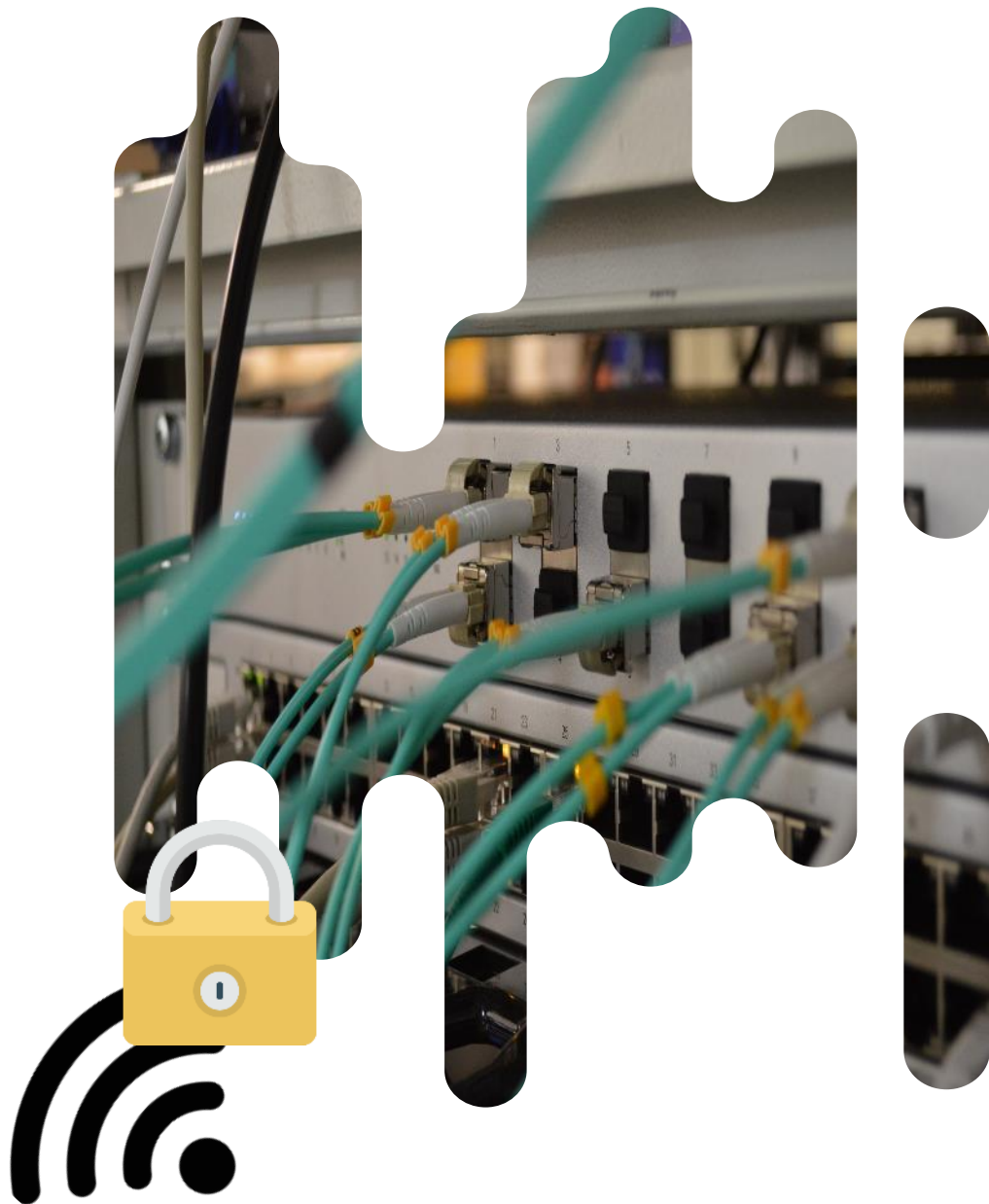
## 7.4. Seguridad en redes Wireless. Redes abiertas



# Redes inalámbricas **privadas**

Un usuario además de conectarse a su red doméstica se conectará habitualmente a otras redes de amigos o corporativas. Muchas de estas serán privadas pero, aun así, no sabemos que tipos de seguridad tienen configuradas y, por lo tanto, no sabemos si nuestra información está segura. Es por ello que debemos tomar las mismas medidas que si fueran públicas.





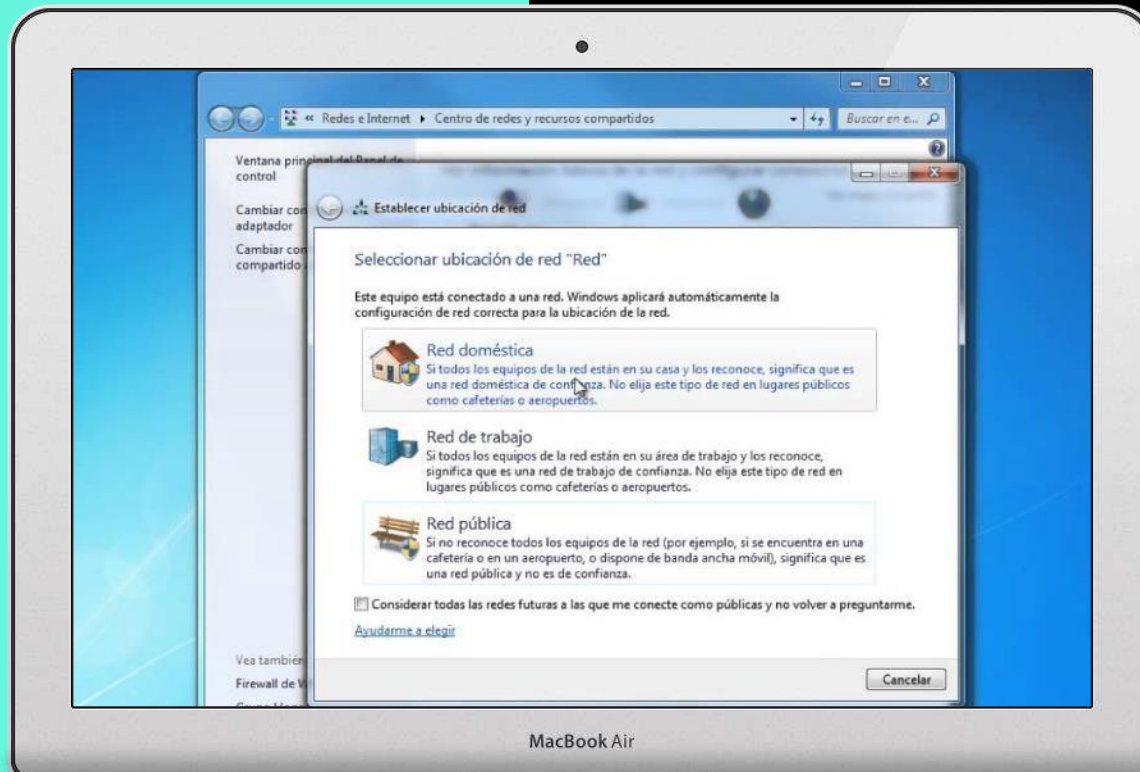
## ¿Cómo identificar una red inalámbrica segura?

Ya lo hemos comentado antes, deberíamos fijarnos en si la conexión a la cual queremos acceder está protegida por contraseña y posteriormente fijarnos en el tipo de cifrado que utiliza: WEP, WPA o WPA2, siendo esta última la más segura y teniendo en cuenta que con las dos anteriores, una persona con los conocimientos suficientes podría estar leyendo toda la información que circule por esa red.

# Redes wifi públicas

Es muy importante tener en cuenta que cuanto te conectas a una red pública, debes ser consciente y no utilizarla para mover archivos o información sensible. Si aún así accedes, debes tener en cuenta que Windows y muchos firewall te preguntarán al acceder de qué tipo de red se trata. Te recomendamos que indiques que es pública para que adopten una configuración más restrictiva.

Se recomienda que si sueles manejar información sensible no accedas a wifis compartidas o públicas.





¡Vamos a ver un resumen del uso correcto del wifi!

## **USO CORRECTO DEL WIFI**



02:06



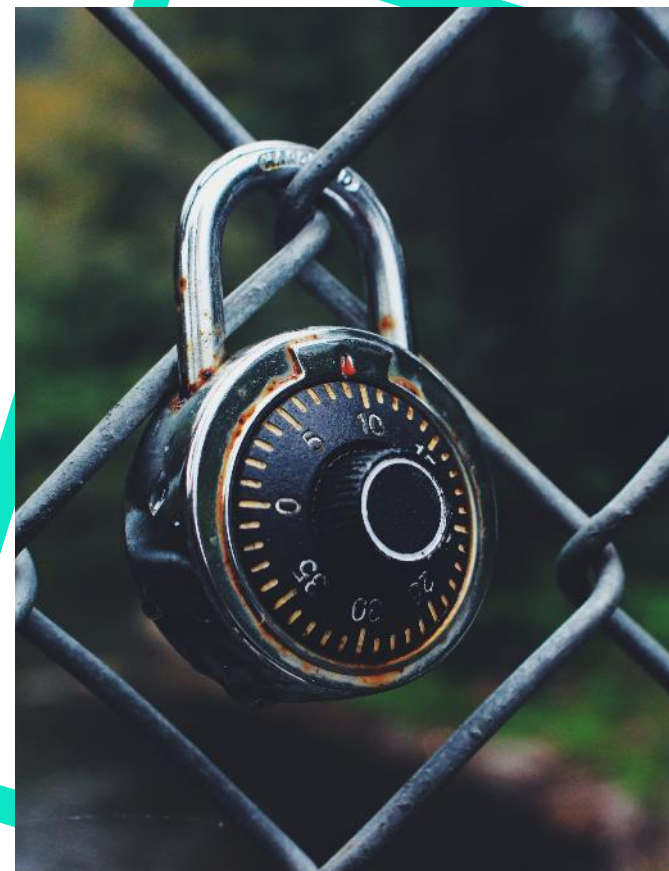




## 7.5. WEP<sup>7</sup>

# WEP

El protocolo WEP (*Wired Equivalent Privacy*) se utiliza como un complemento opcional del estándar IEEE 802.11 a/g/b. Ofrece servicios de acceso a una WLAN para garantizar la confidencialidad de los datos transferidos.



# WEP

## Autenticación WEP

### Autenticación abierta.

Usan solo identificador de red **SSID**, es decir, no usan contraseña, solo un identificador de red inalámbrica. El usuario envía una trama 802.11 que contiene datos de identificación del usuario. El protocolo WEP lo verifica y envía una trama de confirmación o de denegación de acceso a la red inalámbrica.



### Clave compartida.

Usa una clave compartida de 40 bits. Esta será la misma para todos los usuarios de la red. Se distribuye de forma secreta y el proceso de autenticación verifica la identidad del usuario.

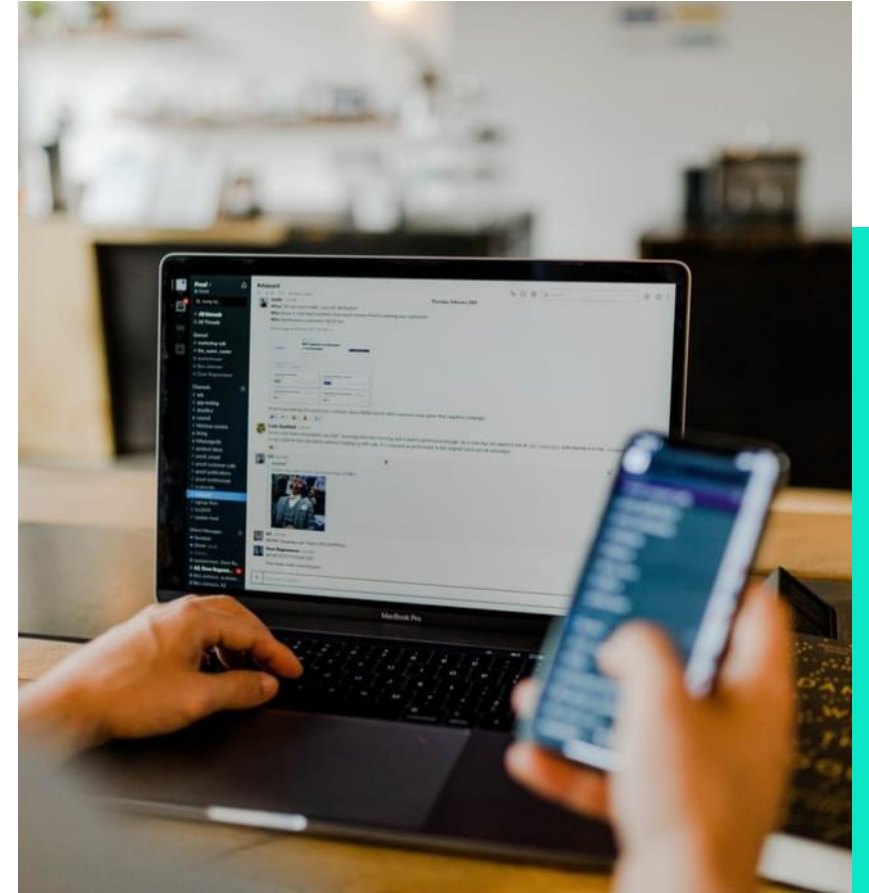


# WEP

## Cifrado WEP

Como ya hemos dicho anteriormente, el **protocolo WEP utiliza el algoritmo de cifrado simétrico RC4, con claves de 64 o 128 bits.**

En 1996 se rompió el algoritmo tal y como se emplea en este protocolo.







## 7.6. WEP. Ataques



Hay que hacer especial hincapié en que el protocolo web no es resistente contra ataques conocidos como:

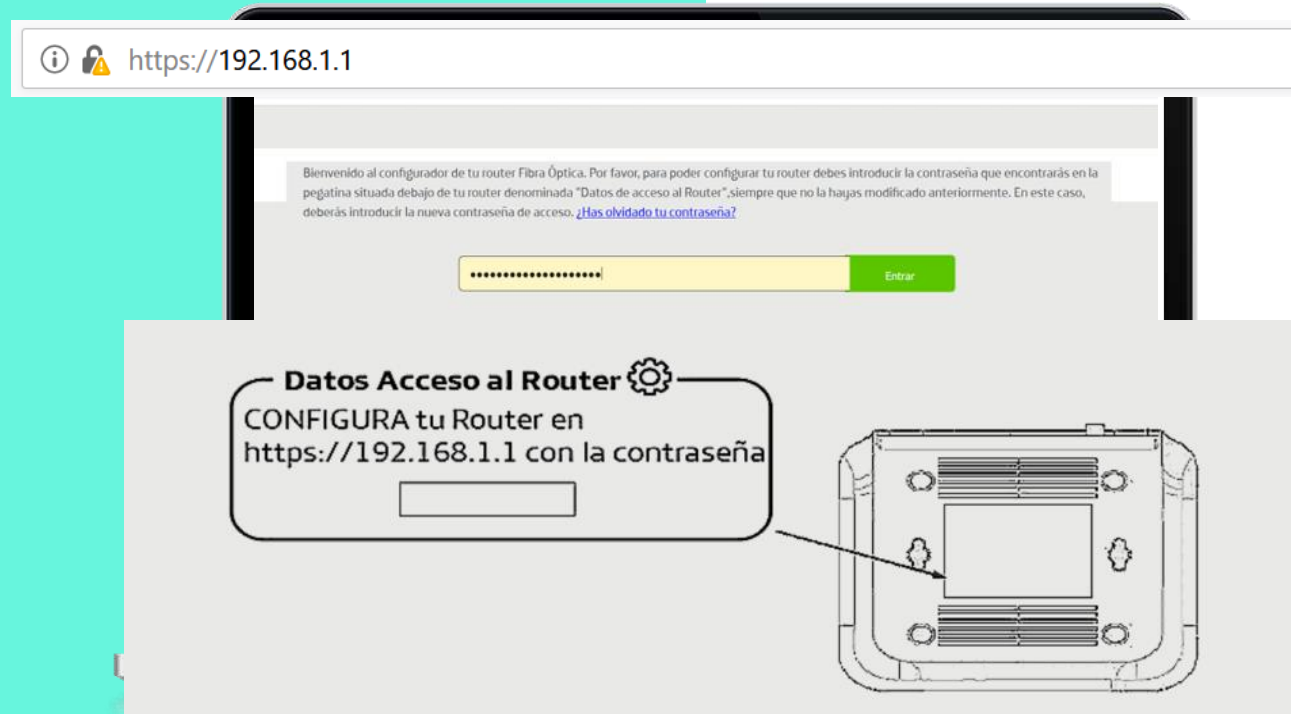
Monitorización de actividad

Ataque de fuerza bruta

Ataque de repetición

# Configuración de seguridad de una red wifi.

Una vez instalado el router, existen 3 configuraciones importantes que debemos realizar en cuanto la red esté instalada.



Para ello, lo primero que haremos será acceder al router a través de una dirección IP tipo, `https://192.168.X.X`. que insertaremos como url en nuestro navegador.

Los datos de acceso los encontrarás normalmente en el manual de instrucciones o, incluso, en la parte inferior de tu router.



## Cambiar las credenciales de acceso.

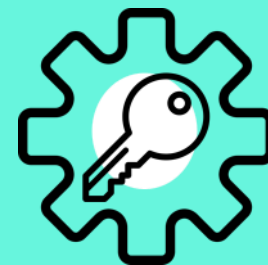
---

Es importante que al acceder por primera vez a tu router cambies los datos de acceso **que vienen de fábrica** por unos nuevos, para evitar el acceso a la configuración por parte de cualquier persona ajena.



## Cambiar la contraseña de acceso a la red.

---



## Configurar el tipo de cifrado de la red.

---

Utilizar el cifrado WPA2 con encriptación AES es lo más seguro para nuestra red de casa. Con ello, lo que conseguimos es que alguien que esté monitoreando datos no pueda acceder a los nuestros porque serán ilegibles.



# Configuración de seguridad avanzada.

Si lo que deseamos es ir un paso por delante en la seguridad de nuestra wifi de casa, será recomendable aplicar las medidas avanzadas que nos permiten ir más allá del cifrado y la protección por contraseña.



## Configurar el firewall.

Esta opción se podrá elegir siempre y cuando nuestro router lo permita. Podremos elegir qué puertos y servicios queremos que estén disponibles para un acceso externo a la red.



## Acceso al router por HTTPS.

Con esta opción, lo que haremos, será configurar nuestro acceso al router a través del protocolo HTTP seguro para evitar que un atacante capture nuestra contraseña de acceso a la configuración.



## Ocultar el SSID (Service Set Identifier) de la red.

Esto es el nombre que identifica a nuestra wifi. Deberemos cambiar el nombre de la misma y ocultarlo para que no aparezca en el listado de redes disponibles.



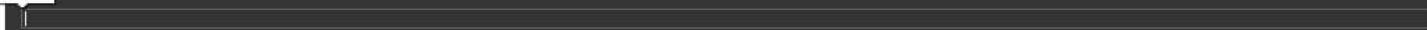
Vamos ver cómo *asegurar tu red local*



**ASEGURA TU RED LOCAL**



01:43





## 7.7. Otros mecanismos de cifrado



## Protocolo WPA

El protocolo WPA (*Wi-Fi Protected Access*), aceptado en 2002, surge a raíz de las vulnerabilidades encontradas en el protocolo WEP.

Este protocolo sirvió de puente hasta la aprobación en 2004 del nuevo estándar IEEE 802.11i.

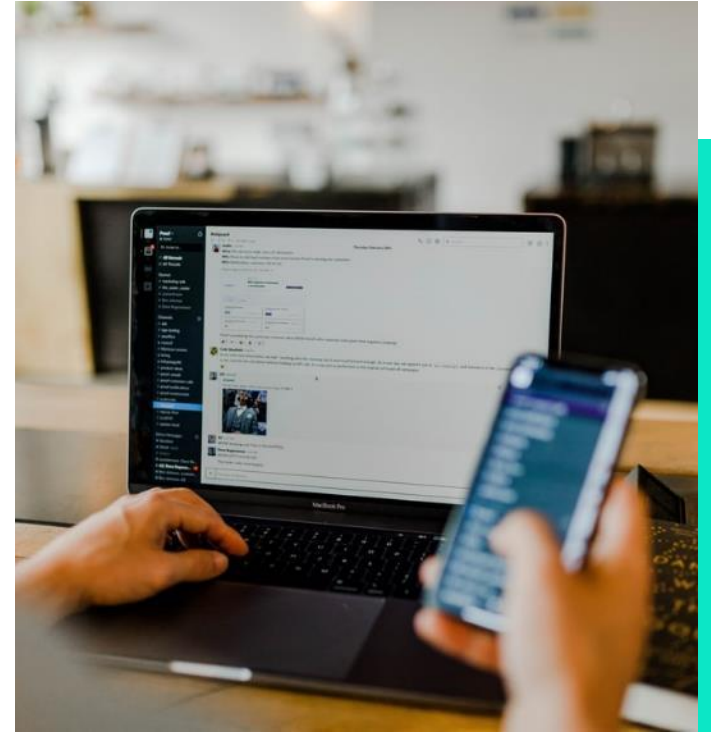
Lo que se hizo fue que el WPA contuviese un subconjunto de las prestaciones de dicho nuevo estándar, de forma que se favoreciese su compatibilidad.

**Sigue utilizando el algoritmo RC4**, pero incorpora nuevos mecanismos de seguridad:

*Temporary Key Integrity Protocol (TKIP).*

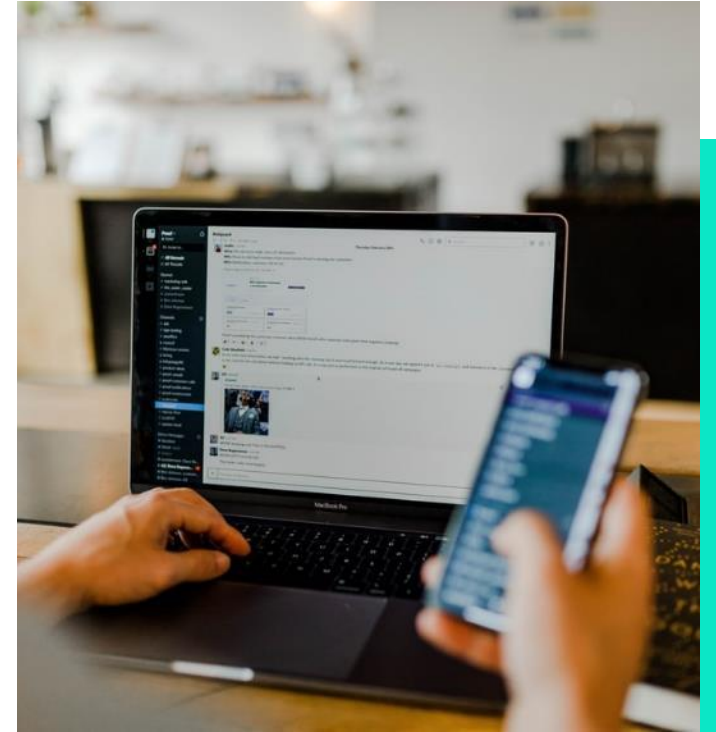
*Message Integrity Check (MIC).*

Control de acceso basado en el estándar 802.1x con el protocolo EAP (*Extensible Authentication Protocol*).



## Protocolo WPA2

- El estándar 802.11i, conocido como WPA2, combina los mecanismos de 802.1x y de TKIP (*Temporary Key Integrity Protocol*).
- El algoritmo que utiliza es AES con longitud de bloque 128 bits.
- Amplía las prestaciones del protocolo WPA como el protocolo CCMP y los mecanismos de preautenticación que permiten que la itinerancia entre puntos de acceso sea rápida y segura.
- Sus principales mecanismos y servicios de seguridad son la confidencialidad, la autenticación y la integridad.





# ¡Enhorabuena!

Has conseguido superar la séptima unidad. Continúa con el curso para... ¡Ser el mejor en gestión de la seguridad informática en tu empresa!